

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-091302

(43)Date of publication of application : 27.03.2002

(51)Int.Cl.

G09C 1/00

G06K 17/00

G06K 19/10

H04L 9/32

(21)Application number : 2000-284052

(71)Applicant : NTT DATA CORP

(22)Date of filing : 19.09.2000

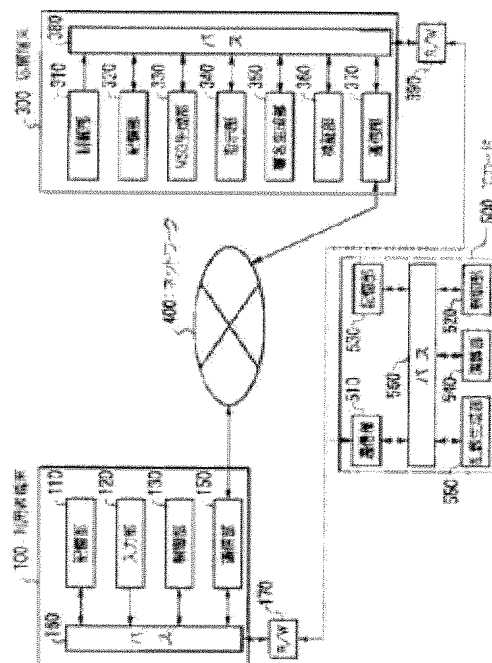
(72)Inventor : TAKAHASHI YOSHIO

## (54) SIGNATURE GENERATION DEVICE, SIGNATURE VERIFICATION DEVICE AND SIGNATURE GENERATION AIDING DEVICE

(57)Abstract:

**PROBLEM TO BE SOLVED:** To provide a signature generation device, a signature verification device and a signature generation aiding device for allowing a customer to perform a temporary signature in a store, and after checking the contents of a contract to be signed, allowing the customer to perform a formal electronic signature.

**SOLUTION:** The signature generation device having a communication means for transmitting/receiving information for performing a signature by an electronic signature in the signature verification device is provided with a storage means for storing secret key information to be the information for performing the signature and an arithmetic means for computing temporary signature information to be information for temporarily signing a message by using the secret key information stored in the storage means and a message to be information concerned with the contents of a document received from the signature verification device by the communication means to perform the electronic signature and conversion data to be information for converting the temporary signature into a signature and characterized by transmitting the temporary signature information to the signature verification device by the communication means, then transmitting conversion data to the signature verification device and performing the signature by the electronic signature.





(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-91302  
(P2002-91302A)

(43) 公開日 平成14年3月27日 (2002.3.27)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テマコード* (参考)
G 0 9 C 1/00	6 4 0	G 0 9 C 1/00	6 4 0 B 5 B 0 3 6
G 0 6 K 17/00		G 0 6 K 17/00	V 5 B 0 6 8
19/10		19/00	S 5 J 1 0 4
H 0 4 L 9/32		H 0 4 L 9/00	6 7 5 D
			6 7 5 C
審査請求 未請求 請求項の数 8 O L (全 12 頁)			

(21) 出願番号 特願2000-284052(P2000-284052)

(22) 出願日 平成12年9月19日 (2000.9.19)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ  
東京都江東区豊洲三丁目3番3号

(72) 発明者 高橋 芳夫

東京都江東区豊洲三丁目3番3号 株式会  
社エヌ・ティ・ティ・データ内

(74) 代理人 100064908

弁理士 志賀 正武 (外2名)

Fターム(参考) 5B035 AA15 BB09 BC01 CA11

5B058 CA27 KA02 KA04 KA06 KA35

KA37 YA20

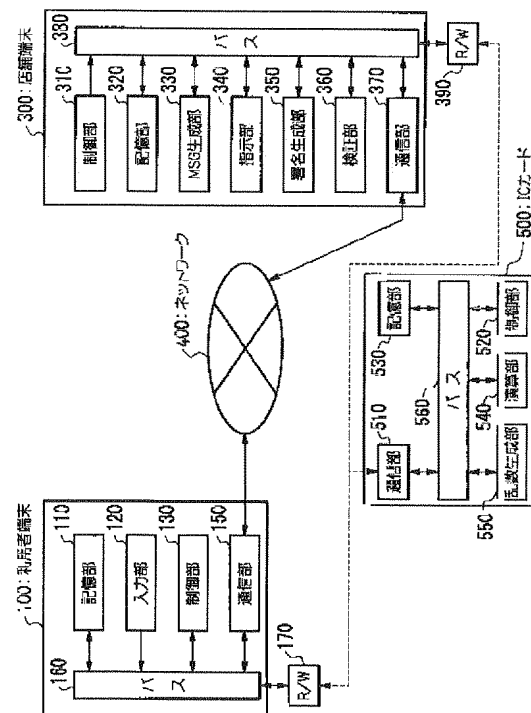
5J104 AA09 LA03 LA06 NA35 NA40

(54) 【発明の名称】 署名生成装置および署名検証装置、署名生成補助装置

(57) 【要約】

【課題】 店頭でタイムリーに仮署名を行い、署名する契約内容を確認した後に正式な電子署名を行うことができる署名生成装置および署名検証装置、署名生成補助装置を提供する。

【解決手段】 署名検証装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名生成装置において、署名を行うための情報となる秘密鍵情報を記憶する記憶手段と、記憶手段に記憶される秘密鍵情報と通信手段によって署名検証装置から受信する電子署名を行う文書の内容に関する情報となるメッセージとを用いてメッセージに仮署名を行うための情報である仮署名情報と仮署名を署名に変換するための情報である変換データを演算する演算手段とを有し、通信手段によって仮署名情報を署名検証装置に送信した後に、変換データを署名検証装置に送信して電子署名によって署名を行うことを特徴とする。



【特許請求の範囲】

【請求項1】 署名検証装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名生成装置において、  
前記署名を行うための情報となる秘密鍵情報を記憶する記憶手段と、  
前記記憶手段に記憶される秘密鍵情報と前記通信手段によって前記署名検証装置から受信する電子署名を行う文書の内容に関する情報となるメッセージとを用いて前記メッセージに仮署名を行うための情報である仮署名情報と前記仮署名を署名に変換するための情報である変換データを演算する演算手段とを有し、  
前記通信手段によって仮署名情報を前記署名検証装置に送信した後に、前記変換データを前記署名検証装置に送信して電子署名によって署名を行うことを特徴とする署名生成装置。

【請求項2】 署名生成装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名検証装置において、  
前記電子署名によって署名を行う文書の内容に関する情報となるメッセージを生成するメッセージ生成手段と、  
前記署名生成装置に記憶される秘密鍵情報と前記メッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報が演算されたか否かを、前記秘密鍵情報に対応する公開鍵情報と前記メッセージとを用いて検出する検証手段と、  
前記検証手段によって、前記仮署名情報が演算されたことが検出された場合に、前記メッセージに対する仮契約として設定する制御手段と、  
前記制御手段によって仮契約が設定された後に、前記署名生成装置から送信される変換データに基づいて、前記仮署名情報から署名情報を演算する署名生成手段と、  
を有することを特徴とする署名検証装置。

【請求項3】 署名検証装置に通信手段によって接続されるとともに、前記署名検証装置と通信を行う署名生成装置に通信手段によって接続され、前記署名検証装置と前記署名生成装置とに対して、電子署名によって署名を行うための情報を送受信する署名生成補助装置において、  
前記署名を行うための情報となる秘密鍵情報が部分秘密鍵情報として2分割され、分割された一方の部分秘密鍵情報を記憶する記憶手段と、  
前記記憶手段に記憶される部分秘密鍵情報と前記署名検証装置から送信される前記電子署名によって署名を行う文書の内容に関する情報となるメッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報と前記仮署名を署名に変換するための情報である変換データを演算する演算手段とを有し、  
前記通信手段によって仮署名情報を前記署名検証装置に送信した後に、前記変換データを前記署名検証装置に送信して電子署名によって署名を行うことを特徴とする署

名生成補助装置。

【請求項4】 署名生成補助装置に通信手段によって接続されるとともに、前記署名生成補助装置と通信を行う署名生成装置に通信手段によって接続され、前記署名生成補助装置と前記署名生成装置とに対して、電子署名によって署名を行うための情報を送受信する署名検証装置において、  
前記電子署名によって署名を行う文書の内容に関する情報となるメッセージを生成するメッセージ生成手段と、  
前記メッセージを前記署名生成装置に送信した後、前記署名生成装置から送信される部分署名情報を記憶する記憶手段と、  
前記メッセージを前記署名生成補助装置に送信した後、前記署名生成補助装置に記憶される部分秘密鍵情報と前記メッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報が演算されたか否かを、前記分割された秘密鍵情報に対応する公開鍵情報と前記メッセージと前記部分署名情報とを用いて検出する検証手段と、  
前記検証手段によって、前記仮署名情報が演算されたことが検出された場合に、前記メッセージに対する仮契約として設定する制御手段と、  
前記制御手段によって仮契約が設定された後に、前記署名生成補助装置から送信される変換データに基づいて、前記仮署名情報から署名情報を演算する署名生成手段と、  
を有することを特徴とする署名検証装置。

【請求項5】 署名検証装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名生成装置における電子署名生成プログラムを記憶した記録媒体において、  
前記記録媒体は、  
前記署名を行うための情報となる秘密鍵情報を記憶する記憶ステップと、  
前記記憶ステップによって記憶される秘密鍵情報と前記通信手段によって前記署名検証装置から受信する電子署名を行う文書の内容に関する情報となるメッセージとを用いて前記メッセージに仮署名を行うための情報である仮署名情報と前記仮署名を署名に変換するための情報である変換データを演算する演算ステップとを有し、  
前記通信手段によって仮署名情報を前記署名検証装置に送信した後に、前記変換データを前記署名検証装置に送信して電子署名によって署名を行う送信ステップと、  
をコンピュータに行わせることを特徴とする署名生成プログラムを記憶した記録媒体。

【請求項6】 署名生成装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名検証装置における署名生成プログラムを記憶した記録媒体において、  
前記記録媒体は、

前記電子署名によって署名を行う文書の内容に関する情報となるメッセージを生成するメッセージ生成ステップと、  
 前記署名生成装置に記憶される秘密鍵情報と前記メッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報が演算されたか否かを、前記秘密鍵情報に対応する公開鍵情報と前記メッセージとを用いて検出する検証ステップと、  
 前記検証ステップによって、前記仮署名情報が演算されたことが検出された場合に、前記メッセージに対する仮契約として設定する制御ステップと、  
 前記制御ステップによって仮契約が設定された後に、前記署名生成装置から送信される変換データに基づいて、前記仮署名情報から署名情報を演算する署名生成ステップと、  
 をコンピュータに行わせることを特徴とする署名生成プログラムを記憶した記録媒体。

【請求項7】 署名検証装置に通信手段によって接続されるとともに、前記署名検証装置と通信を行う署名生成装置に通信手段によって接続され、前記署名検証装置と前記署名生成装置とに対して、電子署名によって署名を行うため情報を送受信する署名生成補助装置における署名生成プログラムを記憶した記録媒体において、  
 前記記録媒体は、  
 前記署名を行うための情報となる秘密鍵情報が部分秘密鍵情報として2分割され、分割された一方の部分秘密鍵情報を記憶する記憶ステップと、  
 前記記憶ステップによって記憶される部分秘密鍵情報と前記署名検証装置から送信される前記電子署名によって署名を行う文書の内容に関する情報となるメッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報と前記仮署名を署名に変換するための情報である変換データを演算する演算ステップと、  
 前記通信手段によって仮署名情報を前記署名検証装置に送信した後に、前記変換データを前記署名検証装置に送信して電子署名によって署名を行う送信ステップと、  
 をコンピュータに行わせることを特徴とする署名生成プログラムを記憶した記録媒体。

【請求項8】 署名生成補助装置に通信手段によって接続されるとともに、前記署名生成補助装置と通信を行う署名生成装置に通信手段によって接続され、前記署名生成補助装置と前記署名生成装置とに対して、電子署名によって署名を行うため情報を送受信する署名検証装置における署名生成プログラムを記録した記録媒体において、  
 前記記録媒体は、  
 前記電子署名によって署名を行う文書の内容に関する情報となるメッセージを生成するメッセージ生成ステップと、  
 前記メッセージを前記署名生成装置に送信した後、前記

署名生成装置から送信される部分署名情報を記憶する記憶ステップと、

前記メッセージを前記署名生成補助装置に送信した後、前記署名生成補助装置に記憶される部分秘密鍵情報と前記メッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報が演算されたか否かを、前記分割された秘密鍵情報に対応する公開鍵情報と前記メッセージと前記部分署名情報とを用いて検出する検証ステップと、

前記検証ステップによって、前記仮署名情報が演算されたことが検出された場合に、前記メッセージに対する仮契約として設定する制御ステップと、  
 前記制御ステップによって仮契約が設定された後に、前記署名生成補助装置から送信される変換データに基づいて、前記仮署名情報から署名情報を演算する署名生成ステップと、

をコンピュータに行わせることを特徴とする署名生成プログラムを記憶した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、電子署名を生成するための秘密鍵の安全な使用方法、署名生成装置および署名検証装置、署名生成補助装置に関するものである。

【0002】

【従来の技術】従来、電子署名を行うための署名用秘密鍵をＩＣカードのような耐タンパー性のある特殊な装置に保管、使用する場合には、ＰＩＮ（個人識別番号）による持ち主の認証、認証局の管理するＣＲＬによる紛失・盗難時の不正対策が行われていた。

【0003】

【発明が解決しようとする課題】しかしながら、従来のＩＣカードには、通常、表示機能がないため、利用者が店頭で契約書などに署名する場合には、契約書の文書内容を店舗のディスプレイで確認したとしても、実際にＩＣカードが署名する契約書の文書とディスプレイに表示されている文書が同一である保証はない。従って、利用者は、何に署名をしているのかを確認できないという問題があった。この問題点を解決するために、ディスプレイ付のＩＣカードが提案されているが、ＩＣカードの製造コストの増加や、ＩＣカードと他の端末機器との互換性が悪いという問題点があった。また、ＩＣカードに設けられたディスプレイでは、画面が小さすぎ、文書を確認することが困難であった。

【0004】また、契約書の内容を確認するために、利用者が契約書に関する情報を記録媒体に記録して自宅に持ち帰り、自宅のコンピュータによって確認した後、署名をすれば安全であるが、その場（店頭など）において契約せずに自宅に戻ってから署名を送信するのでは、その間に他の顧客が先に予約を行ってしまうことによって

損をする可能性があり、利用者としては、安全性を選択するか契約を急ぐかを選択しなければならないという問題があった。さらに、ＩＣカードに秘密鍵を格納して持ち歩く場合、ＩＣカードの紛失、盗難、あるいは利用者が気づかない間に秘密鍵の情報が盗まれる可能性があり、秘密鍵を安全に管理する必要がある。

【０００５】本発明はこのような事情に鑑みてなされたもので、その目的は、店頭でタイムリーに仮署名を行い、署名する契約内容を確認した後に正式な電子署名を行うことができるＩＣカード、店舗端末を提供することにある。

【０００６】

【課題を解決するための手段】上記目的を達成するために、本発明は、署名検証装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名生成装置において、前記署名を行うための情報となる秘密鍵情報を記憶する記憶手段と、前記記憶手段に記憶される秘密鍵情報と前記通信手段によって前記署名検証装置から受信する電子署名を行う文書の内容に関する情報となるメッセージとを用いて前記メッセージに仮署名を行うための情報である仮署名情報と前記仮署名を署名に変換するための情報である変換データを演算する演算手段とを有し、前記通信手段によって仮署名情報を前記署名検証装置に送信した後に、前記変換データを前記署名検証装置に送信して電子署名によって署名を行うことを特徴とする。

【０００７】また、本発明は、署名生成装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名検証装置において、前記電子署名によって署名を行う文書の内容に関する情報となるメッセージを生成するメッセージ生成手段と、前記署名生成装置に記憶される秘密鍵情報と前記メッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報が演算されたか否かを、前記秘密鍵情報に対応する公開鍵情報と前記メッセージとを用いて検出する検証手段と、前記検証手段によって、前記仮署名情報が演算されたことが検出された場合に、前記メッセージに対する仮契約として設定する制御手段と、前記制御手段によって仮契約が設定された後に、前記署名生成装置から送信される変換データに基づいて、前記仮署名情報から署名情報を演算する署名生成手段と、を有することを特徴とする。

【０００８】また、本発明は、署名検証装置に通信手段によって接続されるとともに、前記署名検証装置と通信を行う署名生成装置に通信手段によって接続され、前記署名検証装置と前記署名生成装置とに対して、電子署名によって署名を行うための情報を送受信する署名生成補助装置において、前記署名を行うための情報となる秘密鍵情報が部分秘密鍵情報として２分割され、分割された一方の部分秘密鍵情報を記憶する記憶手段と、前記記憶手

段に記憶される部分秘密鍵情報と前記署名検証装置から送信される前記電子署名によって署名を行う文書の内容に関する情報となるメッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報と前記仮署名を署名に変換するための情報である変換データを演算する演算手段とを有し、前記通信手段によって仮署名情報を前記署名検証装置に送信した後に、前記変換データを前記署名検証装置に送信して電子署名によって署名を行うことを特徴とする。

【０００９】また、本発明は、署名生成補助装置に通信手段によって接続されるとともに、前記署名生成補助装置と通信を行う署名生成装置に通信手段によって接続され、前記署名生成補助装置と前記署名生成装置とに対して、電子署名によって署名を行うための情報を送受信する署名検証装置において、前記電子署名によって署名を行う文書の内容に関する情報となるメッセージを生成するメッセージ生成手段と、前記メッセージを前記署名生成装置に送信した後に、前記署名生成装置から送信される部分署名情報を記憶する記憶手段と、前記メッセージを前記署名生成補助装置に送信した後に、前記署名生成補助装置に記憶される部分秘密鍵情報と前記メッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報が演算されたか否かを、前記分割された秘密鍵情報に対応する公開鍵情報と前記メッセージと前記部分署名情報とを用いて検出する検証手段と、前記検証手段によって、前記仮署名情報が演算されたことが検出された場合に、前記メッセージに対する仮契約として設定する制御手段と、前記制御手段によって仮契約が設定された後に、前記署名生成補助装置から送信される変換データに基づいて、前記仮署名情報から署名情報を演算する署名生成手段とを有することを特徴とする。

【００１０】また、本発明は、署名検証装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名生成装置における電子署名生成プログラムを記憶した記録媒体において、前記記録媒体は、前記署名を行うための情報となる秘密鍵情報を記憶する記憶ステップと、前記記憶ステップによって記憶される秘密鍵情報と前記通信手段によって前記署名検証装置から受信する電子署名を行う文書の内容に関する情報となるメッセージとを用いて前記メッセージに仮署名を行うための情報である仮署名情報と前記仮署名を署名に変換するための情報である変換データを演算する演算ステップとを有し、前記通信手段によって仮署名情報を前記署名検証装置に送信した後に、前記変換データを前記署名検証装置に送信して電子署名によって署名を行う送信ステップとをコンピュータに行わせることを特徴とする。

【００１１】また、本発明は、署名生成装置に対して電子署名によって署名を行うための情報を送受信する通信手段を有する署名検証装置における署名生成プログラムを記憶した記録媒体において、前記記録媒体は、前記電

子署名によって署名を行う文書の内容に関する情報となるメッセージを生成するメッセージ生成ステップと前記署名生成装置に記憶される秘密鍵情報と前記メッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報が演算されたか否かを、前記秘密鍵情報に対応する公開鍵情報と前記メッセージとを用いて検出する検証ステップと、前記検証ステップによって、前記仮署名情報が演算されたことが検出された場合に、前記メッセージに対する仮契約として設定する制御ステップと、前記制御ステップによって仮契約が設定された後に、前記署名生成装置から送信される変換データに基づいて、前記仮署名情報から署名情報を演算する署名生成ステップとをコンピュータに行わせることを特徴とする。

【0012】また、本発明は、署名検証装置に通信手段によって接続されるとともに、前記署名検証装置と通信を行う署名生成装置に通信手段によって接続され、前記署名検証装置と前記署名生成装置とに対して、電子署名によって署名を行うため情報を送受信する署名生成補助装置における署名生成プログラムを記憶した記録媒体において、前記記録媒体は、前記署名を行うための情報となる秘密鍵情報が部分秘密鍵情報として2分割され、分割された一方の部分秘密鍵情報を記憶する記憶ステップと、前記記憶ステップによって記憶される部分秘密鍵情報と前記署名検証装置から送信される前記電子署名によって署名を行う文書の内容に関する情報となるメッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報と前記仮署名を署名に変換するための情報である変換データを演算する演算ステップと、前記通信手段によって仮署名情報を前記署名検証装置に送信した後に、前記変換データを前記署名検証装置に送信して電子署名によって署名を行う送信ステップとをコンピュータに行わせることを特徴とする。

【0013】また、本発明は、署名生成補助装置に通信手段によって接続されるとともに、前記署名生成補助装置と通信を行う署名生成装置に通信手段によって接続され、前記署名生成補助装置と前記署名生成装置とに対して、電子署名によって署名を行うため情報を送受信する署名検証装置における署名生成プログラムを記録した記録媒体において、前記記録媒体は、前記電子署名によって署名を行う文書の内容に関する情報となるメッセージを生成するメッセージ生成ステップと、前記メッセージを前記署名生成装置に送信した後、前記署名生成装置から送信される部分署名情報を記憶する記憶ステップと、前記メッセージを前記署名生成補助装置に送信した後、前記署名生成補助装置に記憶される部分秘密鍵情報と前記メッセージとに基づいて、前記メッセージに仮署名を行うための情報である仮署名情報が演算されたか否かを、前記分割された秘密鍵情報に対応する公開鍵情報と前記メッセージと前記部分署名情報とを用いて検出する

検証ステップと、前記検証ステップによって、前記仮署名情報が演算されたことが検出された場合に、前記メッセージに対する仮契約として設定する制御ステップと、前記制御ステップによって仮契約が設定された後に、前記署名生成補助装置から送信される変換データに基づいて、前記仮署名情報から署名情報を演算する署名生成ステップとをコンピュータに行わせることを特徴とする。

【0014】

【発明の実施の形態】以下、本発明の一実施形態によるICカードおよび店舗端末を図面を参照して説明する。ここでは、ICカードを所有する利用者が、店舗に出向き、電子署名によって取引の契約を行う場合を例として説明する。図1は、この発明の一実施形態による電子署名システムの構成を示す概略ブロック図である。この図において、電子署名システムは、利用者端末100と、店舗端末300と、ネットワーク400と、ICカード500とによって構成される。

【0015】利用者端末100は、記憶部110と、入力部120と、通信部150とがバス160によって接続され、装置各部間で各種データが制御部130の制御に基づいてバス160を介して転送される。この利用者端末100は、例えば、利用者の自宅に設けられる。記憶部110は、電子署名を生成するための鍵情報となる秘密鍵SKと、秘密鍵SKに対応する鍵情報である公開鍵(e, n)と、認証局(CA)が発行する公開鍵(e, n)の所持者を証明するデータとなる公開鍵証明書情報Certとを記憶する。また、記憶部110は、各種データを記憶する。通信部150は、ネットワーク400を介して店舗端末300と通信を行う。入力部120は、利用者端末100を使用する利用者からの入力に応じた信号を出力する。

【0016】さらに、利用者端末100の外部には、ICカード500とバス160の間のデータの送受信を行う入出力装置(以下、「R/W」と称す)170が接続される。さらに、利用者端末100は、周辺機器として表示装置(図示せず)が接続されるものとする。ここで、表示装置とはCRT(Cathode Ray Tube)や液晶表示装置等のことをいう。

【0017】店舗端末300は、制御部310と、記憶部320と、MSG生成部330と、指示部340と、署名生成部350と、検証部360と、通信部370と、バス380とによって構成される。店舗端末300の各部は、バス380によって接続され、制御部310によってデータの転送が制御される。この店舗端末300は、例えば、商品の販売店や、金融機関などの店舗に設けられる。

【0018】記憶部320は、公開鍵(e, n)、部分秘密鍵SKbiを記憶する。また、記憶部320は、各種データを記憶する。MSG生成部330は、契約者となる利用者と契約を結ぶための契約書となるメッセージ

(以下、「MSG」と称す)を生成する。指示部340は、バス380とR/W390を介してICカード500に「0」または「1」の指示を行う。この「0」または「1」の指示は、ランダムに決定される。

【0019】検証部360は、ICカード500から送信される乱数 $r_i$ と乱数データ $R_i$ に基づいて、以下に示すフォーマット関数を用いた(1)式が成立するか否かを検出する。

$$F(r_i)^e = R_i \bmod(n) \cdots \cdots (1)$$

ただし、 $F(r_i)$ は、フォーマット関数であり、識別情報IDなど、固定値や、日付、0と1の連続あるいは繰り返しパターンなどからなるテンプレートに入力データを設定し、冗長性を持たせたものである。このフォーマット関数に、さらに、チェックサムや、CRC等のコードを追加したものであってもよい。

【0020】また、検証部360は、ICカード500から送信される部分署名 $y_i$ とMSG生成部330によって生成されるMSGと、公開鍵 $e$ に基づいて、以下に示す(2)式が成立するか否かを検出する。

$$y_i^e = R_i h(MSG) \bmod(n) \cdots \cdots (2)$$

ここで、この実施形態において用いられるハッシュ関数は、一方方向性ハッシュ関数が使用される。このハッシュ関数のほか、パディング処理などの処理をあわせて行ってもよい。

【0021】署名生成部350は、ICカード500から送信される部分署名 $y_i$ と乱数 $r_i$ に基づいて、以下に示す(3)式によって署名 $S$ を生成する。

$$S = y_i / F(r_i) \bmod(n) \cdots \cdots (3)$$

また、署名生成部350は、生成した署名 $S$ をMSGと公開鍵 $e$ に基づいて、以下に示す(4)式が成立するか否かを検出し、署名 $S$ の検証を行う。

$$S^e = h(MSG) \bmod(n) \cdots \cdots (4)$$

【0022】通信部370は、ネットワーク400を介して利用者端末100と通信を行う。さらに、店舗端末300の外には、バス380とICカード500との間のデータの送受信を行うR/W390が接続される。また、店舗端末300は、周辺機器として入力装置、表示装置等(いずれも図示せず)が接続されるものとする。ここで、入力装置とはキーボード、マウス等の入力デバイスのことをいう。表示装置とはCRT(Cathode Ray Tube)や液晶表示装置等のことをいう。

【0023】ICカード500は、通信部510と、制御部520と、記憶部530と、演算部540と、乱数生成部550、バス560とによって構成される。通信部510は、R/W170を介して利用者端末100と通信を行う。また、通信部510は、R/W390を介して店舗端末300と通信を行う。記憶部530は、利用者端末100から送信される秘密鍵SKを記憶する。また、記憶部530は、乱数 $R_i$ が乱数生成部550に

よって生成される毎に記憶する。演算部540は、店舗端末300から送信されるMSGと記憶部530に記憶される秘密鍵SKとに基づいて、以下に示す(5)式によって署名 $S$ を演算する。

$$S = h(MSG)^{SK} \bmod(n) \cdots \cdots (5)$$

【0024】また、演算部540は、署名 $S$ と乱数生成部550によって生成される乱数 $r_i$ とに基づいて、以下に示す(6)式によって仮署名 $y_i$ を演算する。

$$y_i = F(r_i) S \times \bmod(n) \cdots \cdots (6)$$

【0025】また、演算部540は、乱数生成部550によって生成される乱数 $r_i$ と公開鍵 $e$ とに基づいて、以下に示す(7)式によって乱数データ $R_i$ を演算する。

$$R_i = F(r_i)^e \bmod(n) \cdots \cdots (7)$$

乱数生成部550は、乱数 $r_i$ を生成する。

【0026】制御部520は、ICカード500内の各部の間のデータをバス560を介して転送する制御を行う。また、制御部520は、店舗端末300に乱数データ $R_i$ を送信した後に、店舗端末300から「0」が指示された場合に、乱数 $R_i$ を店舗端末300に送信する制御を行うとともに、店舗端末300から「1」が指示された場合に、演算部540によって生成されて仮署名 $y_i$ を店舗端末300に送信する制御を行う。

【0027】次に、図1の構成における電子署名システムの動作について図2のフローチャートを用いて説明する。まず、利用者は、ICカード500をR/W170に挿入した後に記憶部530に記憶されている公開鍵 $(e, n)$ 、秘密鍵SK、公開鍵証明書情報Certとを転送してICカード500の記憶部530に記憶する。そして、利用者は、ICカード500を携帯して店舗端末300が設置された店舗に出向き、店舗の従業員と取引を行い、契約を行う場合に、契約を行う内容の情報となるメッセージの送信を従業員に依頼する。

【0028】次に、従業員は、契約を行う内容の情報となるMSGを生成する指示を店舗端末300に入力する。店舗端末300のMSG生成部330は、MSGの生成指示をうけて、MSGを生成し、生成したMSGを記憶部530に記憶する。制御部310は、MSG生成部330によって生成されたMSGを表示装置に表示する制御を行う。

【0029】次に、利用者によって表示装置に表示されたMSGを確認した後、ICカード500をR/W390に挿入する。ICカード500がR/W390に挿入されると、制御部310は、ICカード500の記憶部530に記憶されている公開鍵 $(e, n)$ と公開鍵証明書情報Certとを読み出す(ステップS1)。そして、店舗端末300は、読み出した公開鍵 $(e, n)$ と公開鍵証明書情報Certとを記憶部320に記憶した後、表示装置に表示する。従業員は、表示装置に表示された公開鍵 $(e, n)$ と公開鍵証明書情報Certとに

よって公開鍵 ( $e, n$ ) を確認した後 (ステップ S2)、入力装置から MSG を送信する指示を入力する。MSG の送信指示が入力されると、制御部 310 は、記憶部 320 に記憶された MSG を読み出し、IC カード 500 へ転送する (ステップ S3)。

【0030】IC カード 500 に転送された MSG は、記憶部 530 に記憶される。MSG が記憶されると、演算部 540 は、MSG と記憶部 530 に記憶される秘密鍵 SK とに基づいて、(5) 式によって署名 S を生成する (ステップ S4)。次に、演算部 540 は、乱数生成部 550 に乱数  $r_i$  の生成を指示する。乱数生成部 550 は、演算部 540 からの指示に応じて乱数  $r_i$  を生成し (ステップ S5)、演算部 540 に出力するとともに、生成された回数との乱数  $r_i$  を記憶部 530 に記憶する。

【0031】演算部 540 は、乱数生成部 550 から乱数  $r_i$  が出力されると、この乱数  $r_i$  と署名 S とに基づいて、(6) 式によって仮署名  $y_i$  を生成するとともに (ステップ S6)、公開鍵  $e$  と乱数  $r_i$  とに基づいて、(7) 式によって乱数データ  $R_i$  を生成し (ステップ S7)、生成した仮署名  $y_i$  と乱数データ  $R_i$  とを一時保持する。そして、演算部 540 は、生成した乱数データ  $R_i$  を通信部 510 によって店舗端末 300 に送信する (ステップ S8)。

【0032】店舗端末 300 は、IC カード 500 から送信される乱数データ  $R_i$  を受信し、記憶部 320 に記憶する。乱数データ  $R_i$  が記憶された後、指示部 340 は、「0」または「1」を IC カード 500 に指示する。指示部 340 から「0」が指示された場合、IC カード 500 の制御部 520 は、記憶部 320 に記憶されている乱数  $r_i$  を読み出して通信部 510 によって店舗端末 300 に出力する制御を行う。通信部 510 は、制御部 520 からの指示に応じて、乱数  $r_i$  を店舗端末 300 に送信する (ステップ S10)。

【0033】店舗端末 300 は、乱数  $r_i$  を受信すると、検証部 360 によって、乱数  $r_i$  と記憶部 320 に記憶されている乱数データ  $R_i$  に基づいて、上述の (1) 式が成立するか否かを検出する (ステップ S11)。検証部 360 は、(1) が成立する場合に、IC カード 500 が正しい秘密鍵 SK を用いて演算したことを検出する。

【0034】一方、指示部 340 から「1」が指示された場合、IC カード 500 の制御部 520 は、演算部 540 に保持されている仮署名  $y_i$  を読み出して通信部 510 によって店舗端末 300 に出力する制御を行う。通信部 510 は、制御部 520 からの指示に応じて、仮署名  $y_i$  を店舗端末 300 に送信する (ステップ S12)。

【0035】店舗端末 300 は、仮署名  $y_i$  を受信すると、記憶部 320 に記憶したのち、検証部 360 によっ

て、仮署名  $y_i$  と記憶部 320 に記憶されている公開鍵  $e$  と MSG と乱数データ  $R_i$  に基づいて、上述の (2) 式が成立するか否かを検出する (ステップ S12)。検証部 360 は、(2) が成立する場合に、IC カード 500 が正しい秘密鍵 SK を用いて演算したことを検出する (ステップ S13)。

【0036】そして、制御部 310 は、正しい秘密鍵 SK を用いて演算されたことが検証部 360 によって検出されると、さらに、ステップ S5 からステップ S13 までの処理動作を  $k$  回繰り返す制御を行う。 $k$  回繰り返した後、常に正しい秘密鍵 SK を用いて演算されたことが検出された場合、制御部 310 は、 $i$  回 ( $1 \leq i \leq k$ ) に送信された仮署名  $y_i$  を署名 S を生成するための情報として記憶部 320 から抽出し、公開鍵 ( $e, n$ )、公開鍵証明書情報 Cert、MSG を関連づけて記憶部 320 に記憶する (ステップ S15)。そして、制御部 310 は、抽出された仮署名  $y_i$  に対応する回数を示す回数情報  $i$  を IC カード 500 に出力する (ステップ S16)。

【0037】IC カード 500 は、店舗端末 300 から出力された回数情報  $i$  を記憶部 530 に記憶する (ステップ S17)。そして、回数情報が記憶された後、利用者は、IC カード 500 を R/W390 から取り出し、自宅へ戻った後、利用者端末 100 によって IC カード 500 に記憶されている MSG を表示装置に表示させ、MSG の内容を再度確認する (ステップ S18)。そして、利用者によって MSG の内容が確認された後、利用者からの送信指示に応じて、通信部 150 は、ネットワーク 400 を介して IC カード 500 の記憶部 530 に記憶されている、回数情報  $i$  に対応する回数の乱数  $r_i$  を変換データとして店舗端末 300 に送信する (ステップ S19)。

【0038】IC カード 500 から送信される乱数  $r_i$  を受信すると、店舗端末 300 は、署名生成部 350 によって、IC カード 500 から送信される部分署名  $y_i$  と乱数  $r_i$  に基づいて、上述の (3) 式によって署名 S を生成する。次いで、署名生成部 350 は、生成した署名 S を MSG と公開鍵  $e$  に基づいて、上述の (4) 式を用いて署名 S の検証を行う。

【0039】上述したように、検証部 360 が上述の (1) 式と (2) 式とが成立するか否かを検出することによって、店舗端末 300 は、IC カード 500 から署名 S そのものを受信することなく、利用者が秘密鍵 SK を持っていることの確認と、利用者が MSG に対して仮署名のデータを生成していることの確認を行うことができる。これらの確認を行うことによって、仮署名を行い、利用者が MSG を確認した後に、乱数  $r_i$  を送信して、仮署名  $y_i$  を署名 S に変換することができる。

【0040】なお、ここで生成される仮署名  $y_i$  は、第三者にとって正当なものであるか否かを判断できないの

で、正式な電子署名として成立しないので、利用者のリスクを利用者および店舗側に限定できる。

【0041】ここで、図3を用いて、仮署名 $y_i$ について説明する。従来のRSA署名の方法を用いると、 $S^e = h(\text{MSG})$ となるが、上記の方法によれば、仮署名 $y_i$ は、 $y_i^e = R_i \times h(\text{MSG})$ となる。従って、仮署名 $y_i$ を乱数を用いて生成した場合、 $R_i = h(\text{MSG}) / y_i^e$ として乱数データ $R_i$ を演算すると、秘密鍵SKを有していない第三者が仮署名 $y_i$ を生成することが可能となり、第三者が利用者になりすますることが可能になってしまう。

【0042】一方、ICカード500は、店舗端末300から指定される「0」または「1」を予測することができない。もし、店舗端末300から「1」が指示されることが予測できるのであれば、上記のように、予め仮署名 $y_i$ を乱数を用いて生成して乱数データ $R_i$ を演算し、そして乱数データ $R_i$ を送信し、店舗端末300から「1」が指示された後に乱数を用いて生成した仮署名 $y_i$ を送信することによって、店舗端末300における検証が成立する(符号600)。

【0043】しかし、店舗端末300から「0」が指示された場合、乱数データ $R_i$ に対応する乱数 $r_i$ を送信しなければ、店舗端末300の検証が成立しない。この場合、 $F(r_i)^e = R_i$ を満たす乱数 $r_i$ を計算することになるが、この乱数 $r_i$ を求めるには、 $r_i = F^{-1}(R_i^{SK})$ という演算を行う必要があり、秘密鍵SKがないと、乱数 $r_i$ を演算できない。従って、ICカード500において「1」が指示されることを予測して乱数 $r_i$ と乱数データ $R_i$ を生成していた場合、秘密鍵SKがないと乱数 $r_i$ を演算できないので、検証部360の検証によって、なりすましを検出することが可能である(符号601)。(ただし、 $F^{-1}()$ は、 $F()$ の逆関数)

【0044】他方、店舗端末300から「0」が指示されることを予測して乱数 $r_i$ を生成して乱数データ $R_i$ を $R_i = F(r_i)^e$ によって生成しておき、乱数データ $R_i$ を店舗端末300に送信した後に、予測どおり店舗端末300から「0」が指示された場合、乱数 $r_i$ を送信すれば、検証部360における検証が成立し、秘密鍵SKを有していない第三者が成りすますることが可能である(符号602)。

【0045】しかし、この場合、店舗端末300から「1」が指示されると、仮署名 $y_i$ を送信しなければならないが、このとき、仮署名 $y_i$ を生成するには、秘密鍵SKが必要となり、秘密鍵SKを有していない第三者は、検証を成立させるための仮署名 $y_i$ を生成することができない(符号603)。従って、検証部360によって、秘密鍵SKを有していない第三者の成りすましを検出することが可能である。

【0046】このように、店舗端末300は、乱数デー

タ $R_i$ を受信した後に「0」または「1」を指示することによって、秘密鍵SKを有する利用者であるか否かを検出することができる。このとき、上述した「0」または「1」の指示を行って、送信されるデータを検証することによって、1回あたり1/2の確率で秘密鍵SKを有していない第三者の成りすましを検出することが可能であるので、「0」または「1」の指示を行う処理をk回繰り返して行うことによって、 $(1/2)^k$ の確率で秘密鍵SKを有していない第三者の成りすましを検出することが可能であるので、店舗端末300は、圧倒的な確率で仮署名 $y_i$ が正しいことを確認することが可能である。従って、店舗端末300は、署名SそのものをICカード500から送信されなくても、秘密鍵SKを有する利用者であることが確認できる。

【0047】店舗端末300における店舗が不正をして仮署名 $y_i$ を偽造した場合、利用者は、仮署名の検証処理を行うことによって仮署名 $y_i$ が偽造されたものであるか否かを検証することが可能である。この検証処理は、例えば、MSGと検証する仮署名 $y_i$ とを入力として、 $T = y_i \div h(\text{MSG})^{SK} \bmod(n)$ なる式によって、仮署名 $y_i$ が $F()$ のフォーマット関数に適合するか否かを検証を行う。このフォーマット関数には冗長性があるので、仮署名 $y_i$ が偽造されている場合、圧倒的に高い確率でフォーマットに適合せず、仮署名 $y_i$ の検証を行うことが可能である。ただし、この検証処理を行う場合、TからMSGに対する署名Sを演算できるため、店舗端末300に直接Tを渡すのではなく、信頼できる第三者がTを確認するようにすることが望ましい。

【0048】次に、第2の実施形態について説明する。図4は、第2の実施形態における電子署名システムの構成を示す概略ブロック図である。この図において、図1の各部に対応する部分には同一の符号を付け、その説明を省略する。利用者端末100の分散部140は、秘密鍵SKを部分秘密鍵SK1と部分秘密鍵SK2とに分割する。乱数生成部180は、乱数 $r_i$ を生成する。演算部190は、図1の演算部540と同様に演算を行い、部分署名S1、乱数データ $R_i$ 、仮署名 $y_i$ を算出する。

【0049】ICカード500の演算部541は、店舗端末300から送信されるMSGと記憶部530に記憶される秘密鍵SK2とに基づいて、以下に示す(8)式によって部分署名S2を演算する

$$S2 = h(\text{MSG})^{SK2} \bmod(n) \dots\dots (8)$$

ここで、部分署名とは、部分署名Snを2つすなわち部分署名S1と部分署名S2とを集めた場合に、署名Sが生成されるものである。

【0050】次に、図4の構成における装置の動作について、図5のフローチャートを用いて説明する。まず、利用者は、ICカード500をR/W170に挿入した後に記憶部530に記憶されている公開鍵(e, n)、公開鍵証明書情報Certとを転送してICカード50

0の記憶部530に記憶する(ステップS48)。次いで、利用者は、入力部120から秘密鍵SKを分割する指示を入力する。分散部140は、入力部120から入力される指示に応じて、記憶部110から秘密鍵SKを読み出し、秘密鍵SK1と秘密鍵SK2とに分割し(ステップS49)、分割した秘密鍵SK1と秘密鍵SK2とを記憶部110に記憶する。分散部140によって秘密鍵SKが分割されると、分割された秘密鍵SK2をICカード500の記憶部530に記憶する(ステップS50)。

【0051】そして、利用者は、ICカード500を携帯して店舗端末300が設置された店舗に出向き、店舗の従業員と取引を行い、契約を行う場合に、契約を行う内容の情報となるメッセージの送信を従業員に依頼する。そして、図2におけるステップS1～ステップS3と同様に、ICカード500から公開鍵(e, n)と公開鍵証明書情報Certとが店舗端末300に送信される(ステップS51)、店舗端末300において公開鍵(e, n)の確認がなされた後(ステップS52)、MSGが生成され、ICカード500に送信される(ステップS53)。

【0052】演算部540は、店舗端末300から送信されるMSGと記憶部530に記憶される秘密鍵SK2とに基づいて、 $S2 = h(MSG)^{SK2} \bmod(n)$ なる式によって部分署名S2を演算し、記憶部530に記憶する。記憶部530に記憶された後、制御部520は、通信部510によって部分署名S2を店舗端末300に送信する(ステップS54)。店舗端末300は、ICカード500から送信される部分署名S2を記憶部530に記憶する。

【0053】部分署名S2が記憶された後、店舗端末300は、MSGを利用者端末100に送信する(ステップS55)。利用者端末100は、演算部190によって部分署名S1を $S1 = h(MSG)^{SK1} \bmod(n)$ なる式によって生成し(ステップS56)、記憶部110に記憶する。次いで、利用者端末100は、乱数生成部180によって乱数 $r_i$ を発生させた後、記憶部110に記憶するとともに、演算部190によって仮署名 $y_i$ と乱数データ $R_i$ と生成して記憶部530に記憶した後、乱数データ $R_i$ を店舗端末300に送信する(ステップS57)。

【0054】店舗端末300は、乱数データ $R_i$ を受信して記憶部320に記憶した後、指示部340によって「0」または「1」を利用者端末100に指示する(ステップS58)。利用者端末100は、店舗端末300から「0」が指示された場合に乱数 $r_i$ を店舗端末300に送信し、「1」が指示された場合に仮署名 $y_i$ を店舗端末300に送信する(ステップS59)。

【0055】店舗端末300は、検証部360によって利用者端末100から送信されるデータに応じて、乱数

$r_i$ または仮署名 $y_i$ を検証する(ステップS60)。そして、上述のステップS57からステップS60までの処理をk回繰り返す(ステップS61)。このとき、店舗端末300は、仮署名 $y_i$ と公開鍵(e, n)と公開鍵証明書情報CertとMSGと部分署名S2とを繰り返した回数 $i$ ( $1 \leq i \leq k$ )に関連づけて記憶部320に記憶する(ステップS61)。そして、店舗端末300は、回数 $i$ を回数情報 $i$ として利用者端末100に送信する(ステップS62)。利用者端末100は、店舗端末300から回数情報 $i$ を受信すると、回数情報 $i$ を記憶部110に記憶する(ステップS63)。

【0056】そして、利用者は、ICカード500を自宅に持ち帰った後、利用者端末100の表示装置にMSGの内容を表示させ、MSGの内容を確認した後、MSGに問題がなければ、回数情報 $i$ に対応する乱数 $r_i$ を変換データとして店舗端末300に送信する(ステップS64)。店舗端末300は、署名生成部350によって利用者端末100から送信された乱数 $r_i$ を用いて $S = (y_i \times S2) \div F(r_i) \bmod(n)$ なる式によって署名Sを生成し、この署名Sを検証部360によって検証する(ステップS65)。

【0057】なお、上記実施形態において、仮署名の生成と乱数 $r_i$ との送信において、ICカード500にPINを設定してもよく、また、このPINをそれぞれ別のデータを設定するようにしてもよい。また、仮署名生成時においてはPINを設定せず、乱数 $r_i$ の送信時においてPINを入力するように設定してもよい。このように、ICカード500のアクセス制御機能を利用して、異なったレベルの制限を設定し、仮署名時に店舗端末300によって乱数 $r_i$ を密に取り出されることを防止することが好ましい。

【0058】なお、上記実施形態において、利用者が乱数 $r_i$ を所定の期間内に送信しなかった場合、店舗端末300は、仮署名 $y_i$ による仮契約を取り消すようにしてもよい。また、上記実施形態において、「0」または「1」を指示して検証部360によって検証を行う処理をk回繰り返すようにしたが、一度にk個のデータを送受信するようにしてもよい。

【0059】また、上記実施形態において、乱数 $r_i$ を生成する場合に、まず乱数 $r_0$ を生成し、 $r_i = h(r_0 \parallel i)$ として生成するようにしてもよい。これにより、1つの乱数 $r_0$ と回数情報 $i$ を記憶しておくことによって、乱数 $r_i$ を算出することが可能であるので、乱数 $r_i$ を生成する毎に記憶する必要がなくなる。これにより、必要な記憶領域の増加を抑えることが可能である。

【0060】さらに、上述した実施形態によれば、従来のRSA署名による方法とほぼ同じ処理を実装すればよいので、ICカードにおける処理を増加させることがなく、これにより、従来のICカードに本発明を適用することができる。

【0061】また、乱数 $r_i$ を $r_i' = h(r_i)$ なる式に代入し、算出される乱数 $r_i'$ を新たな乱数 $r_i$ として、再度上記の式を用いてさらに $r_i'$ を算出するようにしてもよい。また、乱数 $r_i$ の生成は、上述の方法以外によって生成するようにしてもよい。

【0062】なお、上述の第2の実施形態において、秘密鍵SKを2つに分割したが、シークレットシェアを用いて分割するようにしてもよい。ここでいうシークレットシェアは、秘密鍵SKを、しきい値 $k$ で $n$ 個の部分秘密鍵SK1～SK $n$ に分散し、分散された部分秘密鍵SK1～SK $n$ とMSGとに基づいて、部分署名S1～S $n$ が生成する。そして、部分署名S1～S $n$ のうち、任意の部分署名S $n$ が $k$ 個集まった場合に、署名Sが生成されるものである。

【0063】さらに、上述の第2の実施形態において、秘密鍵SKを2つに分割し、ICカード500と利用者端末100とに記憶するようにしたので、ICカード500に紛失、盗難される等の場合が発生しても、利用者端末100によって秘密鍵SKから新たな秘密鍵SK1'と秘密鍵SK2'を生成し、利用者端末100に秘密鍵SK1'を設定すれば、第三者が紛失したICカード500を悪用しようとしても、使用できなくなる効果が得られる。

【0064】さらに、上述の第2の実施形態において、秘密鍵SKを2つに分割した場合を一例として説明したが、秘密鍵SKを秘密鍵SK1と秘密鍵SK2と秘密鍵SK3に分割し、秘密鍵SK1を利用者端末100、秘密鍵SK2をICカード500、秘密鍵SK3を店舗端末300に記憶させ、これら3つの秘密鍵が集まったときに署名Sを生成できるようにしてもよい。

【0065】さらに、上述の第2の実施形態において、秘密鍵SK2が利用者が気づかないうちに第三者にコピーされたとしても、利用者端末100から乱数 $r_i$ を送信しない限り、契約が成立しないので、悪意ある第三者の悪用を防ぐことが可能である。

【0066】また、図1における各部の機能を実現するためのプログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたプログラムをコンピュータシステムに読み込ませ、実行することにより電子署名生成管理を行ってもよい。なお、ここでいう「コンピュータシステム」とは、OSや周辺機器等のハードウェアを含むものとする。また、「コンピュータシステム」は、WWWシステムを利用している場合であれば、ホームページ提供環境（あるいは表示環境）も含むものとする。また、「コンピュータ読み取り可能な記録媒体」とは、フロッピーディスク、光磁気ディスク、ROM、CD-ROM等の可搬媒体、コンピュータシステムに内蔵されるハードディスク等の記憶装置のことをいう。さらに「コンピュータ読み取り可能な記録媒体」とは、インターネット等のネットワークや電話回線等の通

信回線を介してプログラムを送信する場合の通信線のように、短時間の間、動的にプログラムを保持するもの、その場合のサーバやクライアントとなるコンピュータシステム内部の揮発性メモリのように、一定時間プログラムを保持しているものも含むものとする。また上記プログラムは、前述した機能の一部を実現するためのものであっても良く、さらに前述した機能をコンピュータシステムにすでに記録されているプログラムとの組み合わせで実現できるものであっても良い。以上、この発明の実施形態を図面を参照して詳述してきたが、具体的な構成はこの実施形態に限られるものではなく、この発明の要旨を逸脱しない範囲の設計等も含まれる。

【0067】

【発明の効果】以上説明したように、この発明によれば、仮署名情報によって仮契約を行った後に仮署名情報を署名情報に変換する変換データを送信するようにしたので、仮署名を行うことによって秘密鍵が利用者の公開鍵に対応するものであることが確認でき、これにより、契約時に、利用者が実際に契約する本人であることの証明と、仮に契約を結ぶ仮契約を行うことができる効果が得られる。そして、利用者から店舗に変換データを送信することによって仮署名情報を電子署名に変換して契約を行うことができる、店頭でタイムリーに仮署名を行い、署名する契約内容を確認した後に正式な電子署名を行うことができる効果が得られる。

【0068】また、この発明によれば、仮署名した後に電子署名を行うようにしたので、ICカードにディスプレイ等を設けることなくメッセージを確認することができるので、ICカードの製造コストの増加を抑えることができる。また、この発明によれば、仮署名した後に電子署名を行うようにした。従って、電子署名を生成した後は、従来の電子署名情報と同様に扱うことができるので、ICカードと他の端末機器との互換性を低下させることがなく電子署名を行うことができる効果が得られる。

【0069】また、この発明によれば、秘密鍵情報を2つに分割し、ICカードと利用者端末とに記憶するようにしたので、ICカード500に紛失、盗難等が発生した場合に、ICカードの部分秘密鍵が利用者が気づかないうちに第三者にコピーされたとしても、利用者端末から変換データを送信しない限り、契約が成立しないので、秘密鍵情報の機密性を向上させることができる効果が得られる。

【図面の簡単な説明】

【図1】 この発明の一実施形態による電子署名システムの構成を示す概略ブロック図である。

【図2】 図1の構成における電子署名システムの動作について説明するためのフローチャートである。

【図3】 仮署名 $y_i$ について説明するための図面である。

【図4】 第2の実施形態における電子署名システムの構成を示す概略ブロック図である。

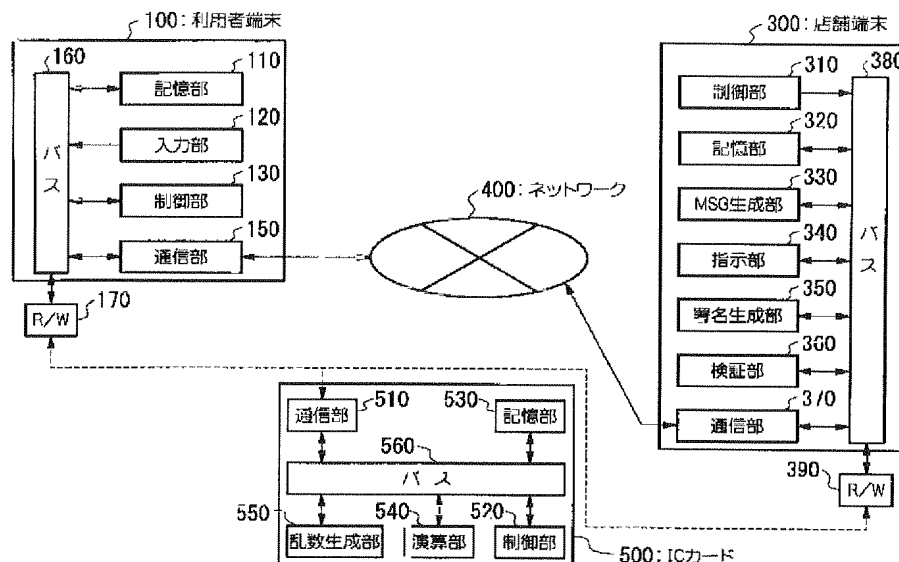
【図5】 図4の構成における電子署名システムの動作について説明するためのフローチャートである。

【符号の説明】

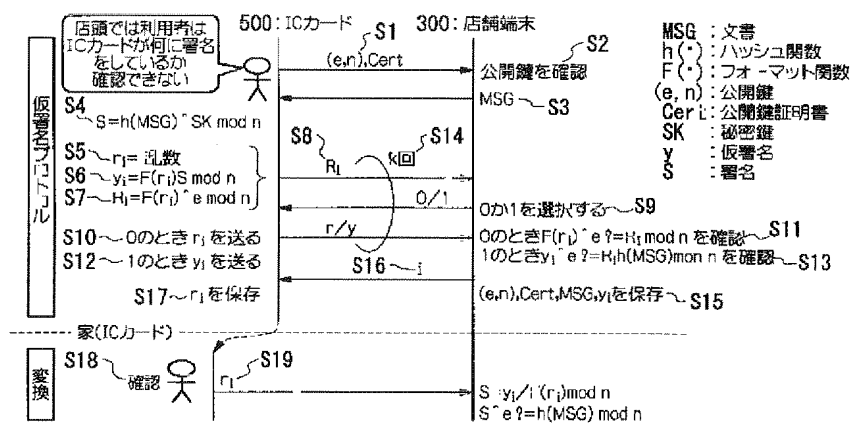
100 利用者端末、 110 記憶部、130、3  
10、520 制御部、 140 分散部、150、3

70、510 通信部、 180 乱数生成部、190 演算部、 300 店舗端末、 320 記憶部、330 MSG生成部、 340 指示部、 350 署名生成部、360 検証部、 500 ICカード、 530 記憶部、540、541 演算部、 550 乱数生成部

【例 1】



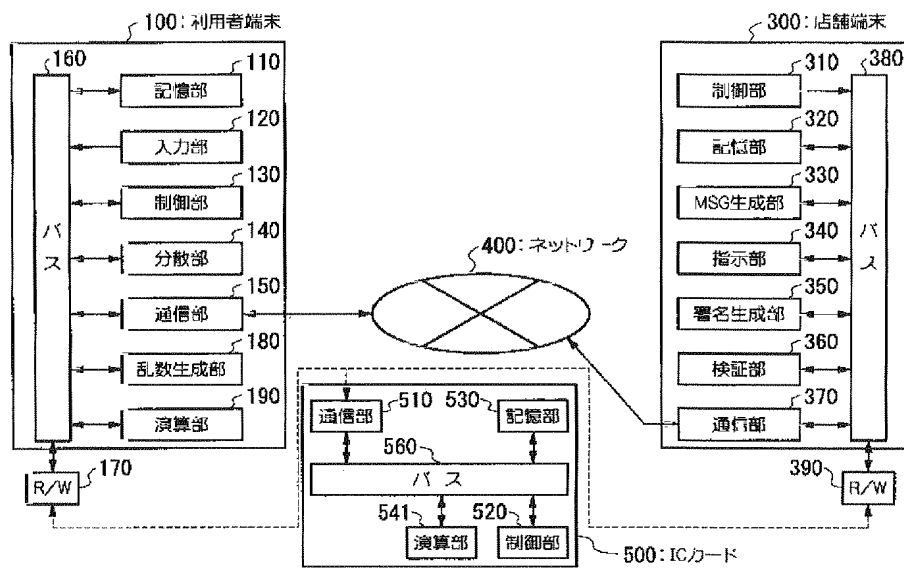
【図2】



【図3】

	Rの生成	検証者が0を選択	検証者が1を選択
ケース0	$r$ : 乱数 $R = r(r)^{e-1}$ $R$ を送信する	$r$ を送る スル成功	$r$ を送るには、 $M$ に対する署名を生成することが必要(秘密鍵が必要)
ケース1	$r$ : 乱数 $R = h(MSG)/y^e$ $R$ を送信する	$r$ を送るには、 $R$ に対する署名を生成することが必要(秘密鍵が必要)	$y$ を送る スル成功

【図4】



【図5】

